Keeping your information safe

by Jacob Bustad

We live in the "Information Age"—with more information about more subjects available to more people than ever before. The benefits are easy to see: improved communication and opportunities for learning. However, the digital world has risks, with the potential for serious consequences like identity theft, data theft, and other types of computer crime. But, just like locking your front door at night, a few simple steps can help keep you ahead of any potential wrongdoers. Julie Fugett, Information Technology Security Analyst at the University of Kansas, offers the following suggestions and sources:

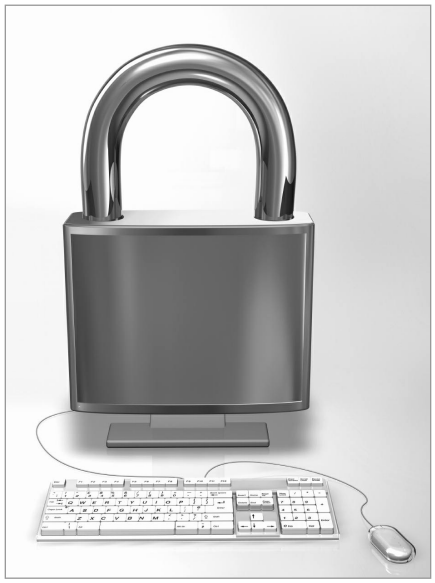
Top ways to be safe, online (and off):

Offline:

• Buy and use a shredder. Crosscut is best! Strip cut is okay if you're on a budget.

• Sensitive data should never go into the trash or recycle bins intact. Dumpsters are gold mines for identity thieves and "social engineers"—those who want to manipulate people into doing something or divulging confidential information. Company phone directories, blueprints, customer and employee records, and other sensitive information should all be put through a shredder prior to being discarded.

• Did you know it is legal for dumpster divers to dig through unlocked dumpsters? If possible, consider locking your dumpsters or trash barrels to deter thieves (for an example of a locking mechanism, check out www.seriouslock.com).



Online:

• Use a firewall.

• Whether it's host-based (software that runs on your computer), network-based (a stand-alone appliance plugged into your network), or both, you should use a firewall to protect your computers, printers, and other devices on your network.

• Antivirus software is not optional. You need it! Install antivirus software and keep it updated. If budgetary constraints are an issue, there are even some excellent free options available (see sidebar for more details).

• Install updates for your operating system and for your other software.

• It's not enough to keep your OS up to date-these days you need to make sure everything from your Office suite to your Web browser to your music software is patched. The reason it's important to keep your OS and installed software up to date is patching security holes. Every day both good guys and bad guys are working to find security holes in operating systems as well as other programs you may install on your computer. If the bad guys find a hole, they write a virus to exploit it. That virus may allow the bad guys to wreak havoc with your computer! Keeping those holes patched will help protect you from viruses and malware designed to exploit these vulnerabilities.

Using e-mail:

• You should treat e-mail just as you would a postcard. Messages go across the wire "in the clear," meaning they are not encrypted or scrambled while in transit. This means anyone who plucks your e-mail off the wire can read it very easily! Here are a few things you should never, ever send in e-mail, not even as an attachment:

—credit card numbers
—bank account numbers
—social security numbers
—login names and passwords

Dumpsters are gold mines for identity thieves and "social engineers"—those who want to manipulate people into doing something or divulging confidential information.

—any information deemed confidential or sensitive by your agency's management.
• Data you should strongly consider not e-mailing:
—Drivers' license numbers
—Information you would prefer remain private—gossip, rumors, etc.
—Content that may violate company policy or get you in "hot water" with management.

Incident response: What to do and when to do it

Let's say, despite your best efforts, your computer's antivirus software pops up a message and says you're infected, or you suspect there may be something going on with your computer. What to do next?
• If you have an IT department or staff person, call them first.
• Run a full antivirus scan of your hard drive and allow your antivirus software to attempt to clean the infection.
• Use antispyware tools like AdAware and Spybot Search & Destroy to search for problems your antivirus may have missed.
• Use an online scan tool like Trend Micro Housecall at http://housecall.trendmicro.com to do a scan as well.
• If you're still having problems, the people who post on the "CastleCops" forums at www.castlecops.com may be able to help you. ▲

Where can I find free antivirus software?

According to KU's Julie Fugett, there is no shortage of options when it comes to antivirus software, both free and for purchase. However, two free software programs she strongly recommends are:

AVG — http://free.grisoft.com/ **Avast!** — http://www.avast.com/

Fugett said: "There are other free antivirus options out there, but they may come bundled with undesirable features and may even venture firmly into 'spyware' territory. AVG and Avast! do not do that."

Further reading...

Microsoft Security at Home blog: http://www.microsoft.com/protect/default.mspx
This site offers security tips and information for both personal and business users of Microsoft products. The blog serves as an up-to-date informational source, commenting on certain security issues and solutions.

OnGuard Online: http://onguardonline.gov/
This site provides practical tips from both the federal government and the technology industry about cyber security, including the ability to file a complaint against a known cyberthief or social engineer.

SANS Tip of the Day: http://www.sans.org/tip_of_the_day.php
The SANS Institute's site gives a new technology security tip each day for free, and also offers courses in cybersecurity education (not free).

Stay Safe Online: http://www.staysafeonline.org/
This site is sponsored by the National Cyber Security Alliance, and provides information for users and their families about basic security tips. Includes a list entitled *Top 8 Cyber Security Practices.*

Security Fix by Brian Krebs: http://blog.washingtonpost.com/securityfix/
Cyber security analyst Brian Krebs offers his own blog at this site, which features daily postings about all kinds of cyber-related issues. You can also search his archives for previous postings, including by topic.

Be SeKUre: http://www.besekure.ku.edu
This site is KU's own cyber security blog, maintained by Fugett. It features regular postings, as well as links to some of the other sites on this list.